(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－204361

(43)公開日　平成９年(1997)８月５日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｃ	
	15/00	３３０			15/00	３３０Ｇ	
Ｇ０６Ｋ	17/00			Ｇ０６Ｋ	17/00	Ｅ	
						Ｆ	
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ａ	

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平8－11899

(22)出願日　平成８年(1996)１月26日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(71)出願人　391024515
三菱電機セミコンダクタソフトウエア株式会社
兵庫県伊丹市中央３丁目１番17号

(72)発明者　藤岡　宗三
兵庫県伊丹市中央３丁目１番17号　三菱電機セミコンダクタソフトウエア株式会社内

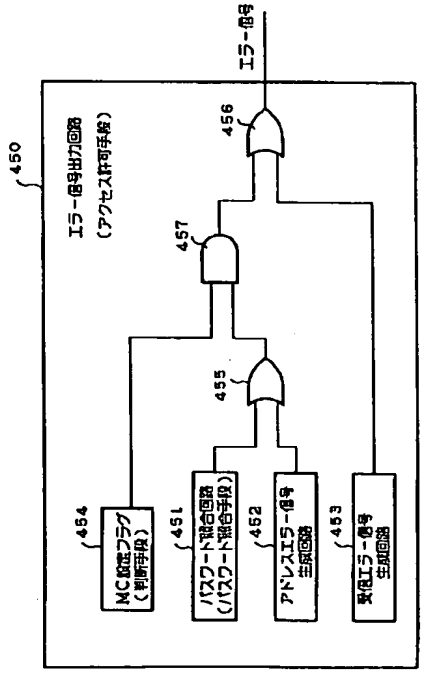
(74)代理人　弁理士　宮田　金雄　（外３名）

(54)【発明の名称】　通信装置

(57)【要約】

【課題】　セキュリティを高くした場合、メモリテストが困難であった。

【解決手段】　製造者コードエリアが設けられたメモリ４０３と、メモリ４０３の製造者エリアＭＡに所定のコードが格納されているときは、パスワードが一致している場合にはリード・ライト装置３００からのユーザエリアＵＡのアクセスを許可し、所定のコードが格納されていない場合には、パスワード照合回路４５１によるパスワードの照合の結果にかかわらずリード・ライト装置３００からのメモリ４０３のメモリ４０３全体へのアクセスを許可するように制御するエラー信号出力回路４５０とを有する非接触式ＩＣカードである。



1

【特許請求の範囲】

【請求項１】　外部装置との間で通信を行う通信装置において、第１の領域と第２の領域とを有するメモリであって、前記第１の領域には前記外部装置が前記メモリをアクセスする際に第１のパスワードの一致が必要であることを示す所定のコードを格納するための第３の領域が設けられているメモリと、前記第３の領域に前記所定のコードが格納されているか否かを判断する判断手段と、前記メモリをアクセスする際に前記外部装置から送られてくる第１のパスワードと前記通信装置の内部に格納されている第１のパスワードとの照合を行うパスワード照合手段と、前記第３の領域に前記所定のコードが格納されているときは、前記パスワード照合手段による照合の結果、第１のパスワードが一致している場合には前記外部装置からの前記メモリの前記第２の領域のアクセスを許可し、前記第３の領域に前記所定のコードが格納されていない場合には、前記パスワード照合手段による第１のパスワードの照合の結果にかかわらず前記外部装置からの前記第１の領域及び前記第２の領域へのアクセスを許可するアクセス許可手段とを具備することを特徴とする通信装置。

【請求項２】　外部装置との間で通信を行う通信装置において、第１の領域と第２の領域とを有するメモリであって、前記第１の領域には前記外部装置が前記メモリをアクセスする際に第１のパスワードの一致が必要であることを示す所定のコードを格納するための第３の領域が設けられているメモリと、前記第３の領域に前記所定のコードが格納されているか否かを判断する判断手段と、前記メモリの前記第３の領域に前記所定のコードが格納されている場合には、前記メモリをアクセスする際に前記外部装置から送られてくる第１のパスワードと前記通信装置の内部に格納されている第１のパスワードとの照合を行うパスワード照合手段と、前記第３の領域に前記所定のコードが格納されているときは、前記パスワード照合手段による照合の結果、第１のパスワードが一致している場合に前記外部装置からの前記メモリの前記第２の領域のアクセスを許可し、前記第３の領域に前記所定のコードが格納されていない場合には、第１のパスワードの照合をせずに前記外部装置からの前記第１の領域及び前記第２の領域へのアクセスを許可するアクセス許可手段とを具備することを特徴とする通信装置。

【請求項３】　判断手段は、第３の領域に所定のコードが格納されているか否かを、外部装置からのＩＤコード要求のコマンドを受信してから前記外部装置にＩＤコードを送出するまでの期間に判断することを特徴とする請求項１または請求項２記載の通信装置。

【請求項４】　第１の領域には第２のパスワードを格納するための第４の領域が設けられており、パスワード照合手段は、第３の領域に所定のコードが格納されている場合に、外部装置から前記第４の領域のアドレスとともに第２のパスワードが送られてきたときには、前記第４の領域に格納されている第２のパスワードと前記外部装置から送られてきた第２のパスワードとを照合し、アクセス許可手段は、前記パスワード照合手段の照合の結果、第２のパスワードが一致した場合には、前記外部装置からの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項１から請求項３のうちのいずれか１項記載の通信装置。

【請求項５】　第１の領域には第２のパスワードを格納するための第４の領域が設けられており、パスワード照合手段は、第３の領域に所定のコードが格納されている場合に、外部装置から前記第４の領域のアドレスとともに第２のパスワードが送られてきたときには、前記第４の領域に格納されている第２のパスワードと前記外部装置から送られてきた第２のパスワードとを照合し、通信装置はさらに前記パスワード照合手段による第２のパスワードの照合の結果、第２のパスワードが一致したときから前記外部装置から送られてくるコマンドの数をカウントするカウント手段を具備し、アクセス許可手段は、前記パスワード照合手段の照合の結果、第２のパスワードが一致し、且つ、前記カウント手段によってカウントされたコマンドの数が所定の数以上である場合に、前記外部装置からの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項１から請求項３のうちのいずれか１項記載の通信装置。

【請求項６】　第１の領域には第２のパスワードを格納するための第４の領域が設けられており、パスワード照合手段は、第３の領域に所定のコードが格納されている場合に、外部装置から前記第４の領域のアドレスとともに第２のパスワードが送られてきたときには、前記第４の領域に格納されている第２のパスワードと前記外部装置から送られてきた第２のパスワードとを照合し、通信装置はさらに前記パスワード照合手段による第２のパスワードの照合の結果、第２のパスワードが一致したときから外部装置から送られてくるコマンドの数をカウントするカウント手段を具備し、アクセス許可手段は、前記パスワード照合手段の照合の結果、第２のパスワードが一致し、且つ、前記カウント手段によってカウントされたコマンドの数が第１の所定数以上で、且つ、第２の所定数以下である場合に、前記外部装置からの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項１から請求項３のうちのいずれか１項記載の通信装置。

【請求項７】　第２のパスワードはメモリからデータを読み出す場合に照合されるリードパスワードと、前記メモリへデータを書き込む場合に照合されるライトパスワードとを含み、第４の領域には前記リードパスワードを格納するためのリードパスワード領域と、ライトパスワ

3

ードを格納するためのライトパスワード領域とが設けられ、パスワード照合手段は、第３の領域に所定のコードが格納されているときに、外部装置からリードパスワード領域のアドレスとともにリードパスワードが送られてきた場合には前記リードパスワード領域に格納されているリードパスワードと前記外部装置から送られてきたリードパスワードとを照合し、前記外部装置から前記ライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合には前記ライトパスワード領域に格納されているライトパスワードと前記外部装置から送られてきたライトパスワードとを照合し、アクセス許可手段は、前記パスワード照合手段による照合の結果、リードパスワードが一致した場合には前記外部装置からの第１の領域及び第２の領域のデータの読み出しを第１のパスワードの照合の一致を必要とせずに許可し、前記パスワード照合手段による照合の結果、ライトパスワードが一致した場合には前記外部装置からの前記第１の領域及び前記第２の領域へのデータの書き込みを第１のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項４から請求項６のうちのいずれか１項記載の通信装置。

【請求項８】　第２のパスワードはメモリからデータを読み出す場合に照合されるリードパスワードと、前記メモリへデータを書き込む場合に照合されるライトパスワードとを含み、第４の領域には前記リードパスワードを格納するためのリードパスワード領域と、前記ライトパスワードを格納するためのライトパスワード領域とが設けられ、パスワード照合手段は、第３の領域に所定のコードが格納されているときに、外部装置から前記リードパスワード領域のアドレスとともにリードパスワードが送られてきた場合には前記リードパスワード領域に格納されているリードパスワードと前記外部装置から送られてきたリードパスワードとを照合し、前記外部装置から前記ライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合には前記ライトパスワード領域に格納されているライトパスワードと前記外部装置から送られてきたライトパスワードとを照合し、アクセス許可手段は、前記パスワード照合手段による照合の結果、リードパスワード及びライトパスワードの両方が一致した場合には前記外部装置からの第１の領域及び第２の領域の読み出し及び書き込みの両方を第１のパスワードの照合の一致を必要とせずに許可することを特徴とする請求項４から請求項６のうちのいずれか１項記載の通信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はプログラマブルメモリを内蔵したＬＳＩを有する非接触式ＩＣカード等の通信装置に関するものである。

【０００２】

4

【従来の技術】図２５は従来の非接触式ＩＣカードに用いられるプログラマブルメモリ内蔵のＬＳＩのメモリマップを示す図である。同図において、１０はメモリ部、１１は書き換え可能なプログラマブルメモリ部、１２は予めデータが書き込まれており書き換えできない固定メモリ部をそれぞれ示している。同図に示すように、プログラマブルメモリ部１１は複数のエリアに分割されている。各エリアにはパスワードが設けられており、各々のエリアをアクセスする場合にはパスワードの照合が行われ、パスワードが一致していない場合にはアクセスが禁止され、パスワードが一致した場合に限りそのパスワードに対応するエリア内のアクセスができるようになっている。

【０００３】このようなＬＳＩでは、ウエハプロセス完了直後はパスワード格納アドレスのデータは不定となり、各エリアをアクセスすることが非常に困難である。このため、ウエハ作成時に固定メモリ部１２にマスタパスワードを書き込んでおき、このマスタパスワードを照合して一致すれば、各エリアのパスワードの照合結果にかかわらず全エリアのアクセスを行えるようにするか、パスワードの変更を許可するようになっている。このマスタパスワードを使用してメモリのテストが行われる。

【０００４】図２６は、従来の非接触式ＩＣカード通信システムの構成を示すブロック図である。同図において、１００はリード・ライト装置、２００は非接触式ＩＣカードを示している。非接触式ＩＣカード２００は、電波を送受信するためのアンテナ２０１と、搬送波をデータで変調するとともに変調された搬送波からデータを復調する変復調回路２０２と、データを格納するプログラマブルメモリ２０３と、非接触式ＩＣカード２００の動作を制御してコマンド処理等を実行する制御回路２０４とを具備している。なお、変復調回路２０２と、プログラマブルメモリ２０３と、制御回路２０４とは非接触式ＩＣカード用のＬＳＩ２１０に組み込まれている。また、プログラマブルメモリ２０３は図２５に示したメモリ部１０と同様の構成となっている。

【０００５】図２７はリード・ライト装置１００と非接触式ＩＣカード２００との間の通信手順を示すシーケンス図である。同図に示すように、まず、リード・ライト装置１００からリードＩＤコマンド（以下ＲＩＤコマンドと記す）が非接触式ＩＣカード２００に送られて通信が開始される。次に、リード・ライト装置１００からコマンドを非接触式ＩＣカード２００に送信する。このコマンドには例えばプログラマブルメモリ２０３のリードやライトなどのコマンドがある。非接触式ＩＣカード２００はこのコマンドを実行し、実行した結果はリード・ライト装置１００に送信される。もしコマンドの実行前に通信エラーやパスワードの照合エラーなどのエラーが生じた場合にはコマンドは実行されずにエラーの状態を示すエラーステータスを送信するか、あるいは、リード

5

・ライト装置１００に何も送信しないようにしている。

【０００６】

【発明が解決しようとする課題】従来の通信装置は以上のように構成されているので、固定メモリに格納されているパスワードがわかってしまうとメモリ全体のデータのアクセスが可能になり、パスワードの変更もできないなどの課題があった。

【０００７】この発明は上記のような課題を解決するためになされたもので、高いセキュリティーを維持しつつ容易にメモリのテストができる通信装置を得ることを目的とする。

【０００８】

【課題を解決するための手段】請求項１記載の発明に係る通信装置は、第１の領域と第２の領域とを有するメモリであって、第１の領域には外部装置がメモリをアクセスする際に第１のパスワードの一致が必要であることを示す所定のコードを格納するための第３の領域が設けられているメモリと、第３の領域に所定のコードが格納されているか否かを判断する判断手段と、メモリをアクセスする際に外部装置から送られてくる第１のパスワードと通信装置の内部に格納されている第１のパスワードとの照合を行うパスワード照合手段と、第３の領域に所定のコードが格納されているときは、パスワード照合手段による照合の結果、第１のパスワードが一致している場合には外部装置からのメモリの第２の領域のアクセスを許可し、第３の領域に所定のコードが格納されていない場合には、パスワード照合手段による第１のパスワードの照合の結果にかかわらず外部装置からの第１の領域及び第２の領域へのアクセスを許可するアクセス許可手段とを具備するものである。

【０００９】請求項２記載の発明に係る通信装置は、第１の領域と第２の領域とを有するメモリであって、第１の領域には外部装置がメモリをアクセスする際に第１のパスワードの一致が必要であることを示す所定のコードを格納するための第３の領域が設けられているメモリと、第３の領域に所定のコードが格納されているか否かを判断する判断手段と、メモリの第３の領域に所定のコードが格納されている場合には、メモリをアクセスする際に外部装置から送られてくる第１のパスワードと通信装置の内部に格納されている第１のパスワードとの照合を行うパスワード照合手段と、第３の領域に所定のコードが格納されているときは、パスワード照合手段による照合の結果、第１のパスワードが一致している場合に外部装置からのメモリの第２の領域のアクセスを許可し、第３の領域に所定のコードが格納されていない場合には、第１のパスワードの照合をせずに外部装置からの第１の領域及び第２の領域へのアクセスを許可するアクセス許可手段とを具備するものである。

【００１０】請求項３記載の発明に係る通信装置は、第３の領域に所定のコードが格納されているか否かを、外部装置からのＩＤコード要求のコマンドを受信してから外部装置にＩＤコードを送出するまでの期間に判断する判断手段を具備するものである。

6

【００１１】請求項４記載の発明に係る通信装置は、第１の領域には第２のパスワードを格納するための第４の領域が設けられたメモリと、第３の領域に所定のコードが格納されている場合に、外部装置から第４の領域のアドレスとともに第２のパスワードが送られてきたときには、第４の領域に格納されている第２のパスワードと外部装置から送られてきた第２のパスワードとを照合するパスワード照合手段と、パスワード照合手段の照合の結果、第２のパスワードが一致した場合には、外部装置からの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【００１２】請求項５記載の発明に係る通信装置は、第１の領域には第２のパスワードを格納するための第４の領域が設けられたメモリと、第３の領域に所定のコードが格納されている場合に、外部装置から第４の領域のアドレスとともに第２のパスワードが送られてきたときには、第４の領域に格納されている第２のパスワードと外部装置から送られてきた第２のパスワードとを照合するパスワード照合手段と、パスワード照合手段による第２のパスワードの照合の結果、第２のパスワードが一致したときから外部装置から送られてくるコマンドの数をカウントするカウント手段と、パスワード照合手段による照合の結果、第２のパスワードが一致し、且つ、カウント手段によってカウントされたコマンドの数が所定の数以上である場合に、外部装置からの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【００１３】請求項６記載の発明に係る通信装置は、第１の領域には第２のパスワードを格納するための第４の領域が設けられたメモリと、第３の領域に所定のコードが格納されている場合に、外部装置から第４の領域のアドレスとともに第２のパスワードが送られてきたときには、第４の領域に格納されている第２のパスワードと外部装置から送られてきた第２のパスワードとを照合するパスワード照合手段と、パスワード照合手段による第２のパスワードの照合の結果、第２のパスワードが一致したときから外部装置から送られてくるコマンドの数をカウントするカウント手段と、パスワード照合手段による照合の結果、第２のパスワードが一致するとともにカウント手段によってカウントされたコマンドの数が第１の所定数以上、且つ、第２の所定数以下である場合に、外部装置からの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【００１４】請求項７記載の発明に係る通信装置は、第

４の領域にはリードパスワードを格納するためのリードパスワード領域と、ライトパスワードを格納するためのライトパスワード領域とが設けられたメモリと、第３の領域に所定のコードが格納されているときに、外部装置からリードパスワード領域のアドレスとともにリードパスワードが送られてきた場合にはリードパスワード領域に格納されているリードパスワードと外部装置から送られてきたリードパスワードとを照合し、外部装置からライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合にはライトパスワード領域に格納されているライトパスワードと外部装置から送られてきたライトパスワードとを照合するパスワード照合手段と、パスワード照合手段による照合の結果、リードパスワードが一致した場合には外部装置からの第１の領域及び第２の領域のデータの読み出しを第１のパスワードの照合の一致を必要とせずに許可し、パスワード照合手段による照合の結果、ライトパスワードが一致した場合には外部装置からの第１の領域及び第２の領域へのデータの書き込みを第１のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【００１５】請求項８記載の発明に係る通信装置は、第４の領域にはリードパスワードを格納するためのリードパスワード領域と、ライトパスワードを格納するためのライトパスワード領域とが設けられたメモリと、第３の領域に所定のコードが格納されているときに、外部装置からリードパスワード領域のアドレスとともにリードパスワードが送られてきた場合にはリードパスワード領域に格納されているリードパスワードと外部装置から送られてきたリードパスワードとを照合し、外部装置からライトパスワード領域のアドレスとともにライトパスワードが送られてきた場合にはライトパスワード領域に格納されているライトパスワードと外部装置から送られてきたライトパスワードとを照合するパスワード照合手段と、パスワード照合手段による照合の結果、リードパスワード及びライトパスワードの両方が一致した場合には外部装置からの第１の領域及び第２の領域の読み出し及び書き込みの両方を第１のパスワードの照合の一致を必要とせずに許可するアクセス許可手段とを具備するものである。

【００１６】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態１．図１はこの実施の形態１の非接触式ＩＣカードの通信システムを示す図であり、図において、３００はリード・ライト装置（外部装置）、４００はリード・ライト装置３００との間で電波を用いて通信を行う非接触式ＩＣカード（通信装置）を示している。非接触式ＩＣカード４００は、電波を送受信するためのアンテナ４０１と、搬送波をデータで変調するとともに変調された搬送波からデータを復調する変復調回路４０２と、データを格納するプログラマブルメモリ（メモリ）４０３と、非接触式ＩＣカード４００の動作を制御してコマンド処理等を実行する制御回路４０４とを具備している。なお、変復調回路４０２と、プログラマブルメモリ４０３と、制御回路４０４とは非接触式ＩＣカード用ＬＳＩ４１０に組み込まれている。

【００１７】図２は非接触式ＩＣカード４００のプログラマブルメモリ４０３のメモリマップを示す図である。図に示すようにアドレスＡＤ０からＡＤ１まではエリアＡ１、アドレスＡＤ１＋１からＡＤ２まではエリアＡ２、アドレスＡＤ２＋１からＡＤ３まではエリアＡ３となっている。エリアＡ４、Ａ５についても同様である。また、エリアＡ１からエリアＡ５にはそれぞれのエリアをアクセスする場合に照合されるパスワード（第１のパスワード）ＰＷ１からＰＷ５がそれぞれ格納されている。なお、エリアＡ１からエリアＡ５はユーザエリア（第２の領域）ＵＡを構成する。また、アドレスＡＤ５＋１からＡＤ６は製造者エリア（第１の領域）ＭＡであり、特定の値が格納されたときにパスワードを有効にする製造者コード（所定のコード、以下ＭＣと記す）を格納するＭＣエリア（第３の領域）が確保されている。なお、ＭＣは、例えば、「００Ｈ」、「０１Ｈ」、「０３Ｈ」、「０７Ｈ」、「０ＦＨ」、「１ＦＨ」、「３ＦＨ」、「７ＦＨ」、「ＦＦＨ」、「８０Ｈ」、「ＣＯＨ」、「ＥＯＨ」、「ＦＯＨ」、「Ｆ８Ｈ」、「ＦＣＨ」、「ＦＥＨ」などのウエハプロセス完了後になりやすいコード、あるいは、製品テストでプログラマブルメモリ４０３に書き込むパターン「００Ｈ」、「ＦＦＨ」、「ＡＡＨ」、「５５Ｈ」は避けて、例えば、「１２Ｈ」、「３４Ｈ」などのコードを用いる。以下の実施の形態ではＭＣとして「１２Ｈ」を用いる場合について説明する。

【００１８】次に動作について説明する。まず、製品テスト時のアクセスについて説明する。製品テストはＬＳＩチップ単体で出荷する場合と非接触式ＩＣカード単位で出荷する場合とでＭＣ設定の時期が異なるが、ここでは非接触式ＩＣカード単位で出荷する場合のテストについて説明する。

【００１９】図３はリード・ライト装置３００と非接触式ＩＣカード４００との間の通信手順を示すシーケンス図である。図に示すように、まずリード・ライト装置３００から非接触式ＩＣカード４００にＩＤ読み出しのＲＩＤコマンドを送信する。非接触式ＩＣカード４００はＲＩＤコマンドを受信するとプログラマブルメモリ４０３内の製造者エリアＭＡのＭＣエリアに特定の値が格納されているか否かを期間Ｐ１の間に確認する。もしＭＣエリアに特定のコード「１２Ｈ」が格納されていれば、それ以降のコミュニケーションにおいてはリード・ライト装置３００からのアクセスはパスワードの照合が必要になる。ＭＣエリアに特定のコード「１２Ｈ」が格納されて

いない場合には、それ以降のリード・ライト装置３００からのアクセスはパスワードの照合の結果が一致していなくても許可される。

【００２０】さて、ＭＣエリアに特定のコード「12H 」が格納されているか否かの確認処理が終了した後、非接触式ＩＣカード４００は自身のＩＤコードをリード・ライト装置３００に送出する。次に、リード・ライト装置３００は非接触式ＩＣカード４００から送られたＩＤコードを確認してコミュニケーションをとるべき相手であると判断されると所定の処理を要求するコマンドを非接触式ＩＣカード４００に送出する。

【００２１】図４はこのコマンドを非接触式ＩＣカード４００が受信したときのエラー処理を実行する制御回路４０４内のエラー信号出力回路（アクセス許可手段）４５０の構成を示す図である。図において、４５１は格納されているパスワードと入力されたパスワードの照合を行い、パスワードが一致しない場合に「H」レベルのパスワードエラー信号を出力するパスワード照合回路（パスワード照合手段）、４５２は非接触式ＩＣカード４００から許可された範囲外のアドレスが指定されたときに「H」レベルのアドレスエラー信号を出力するアドレスエラー信号生成回路、４５３は信号の受信にエラーが生じた場合に「H」レベルの受信エラー信号を出力する受信エラー信号生成回路、４５４はＭＣエリアに特定のコード「12H 」が格納された場合には「H」信号が格納され、その他のコードが格納されている場合には「L」レベル信号が格納されるＭＣ設定フラグ（判断手段）、４５５及び４５６はオアゲート、４５７はアンドゲートである。なお、実際にはＭＣ設定フラグ４５４の値のセットの判断は制御回路４０４によって行われて値がＭＣ設定フラグ４５４に書き込まれる。ＭＣエリアに特定コード「12H 」が書き込まれる前はＭＣエリアには、例えば、「FFH 」等が書き込まれている。このときＭＣ設定フラグ４５４は「L」信号を出力する。このため、アンドゲート４５７ではパスワード照合回路４５１から出力されるパスワードエラー信号及びアドレスエラー信号生成回路４５２から出力されるアドレスエラー信号はマスクされオアゲート４５６からは受信エラーがあった場合にのみ「H」レベルのエラー信号を出力される。このため、パスワードエラー、アドレスエラーが生じた場合であっても受信エラーが生じていなければエラー処理は行われない。従って非接触式ＩＣカード４００のメモリのテスト時にはパスワードが一致しなくてもアドレスＡＤ０からアドレスＡＤ６までの領域をアクセスすることができる。すなわちエラー信号出力回路４５０は外部からのアクセスに対して、そのアクセスを許可するか禁止するかを決定する動作を行う。

【００２２】次に、テストが終了し、ＭＣエリアに特定のコード「12H 」が書き込まれた後はＭＣ設定フラグ４５４に「H」レベル信号が書き込まれ、パスワードエラー信号、アドレスエラー信号、受信エラー信号のうち、いずれか１つの信号が「H」レベルとなったときにオアゲート４５６から「H」レベルのエラー信号が出力される。従って、ＭＣエリアに特定のコード「12H 」が書き込まれた後はパスワードが一致し、且つ、プログラマブルメモリ４０３のアドレスＡＤ０からアドレスＡＤ５の範囲のアドレスを指定したときのみアクセスが許可される。

【００２３】図５はリード・ライト装置３００から非接触式ＩＣカード４００にリードコマンドを転送した場合の通信手順を示すシーケンス図である。また、図６はリードコマンド５１０の構成を示す図である。図６に示すようにリードコマンド５１０はコマンドコード５１１、読み出すデータのアドレス５１２、及びパスワード５１３から構成される。さらに、図７はリードコマンド５１０がリード・ライト装置３００から送信されてきた場合に非接触式ＩＣカード４００からリード・ライト装置３００に送信されるリードデータ５２０の構成を示す図である。図７に示すようにリードデータ５２０はエラーの状態を示すエラーステータス５２１及び読み出したリードデータ列５２２から構成されている。

【００２４】図５に示すように、リード・ライト装置３００から非接触式ＩＣカード４００にＲＩＤコマンドが送られることによってリード・ライト装置３００と非接触式ＩＣカード４００との間のデータ通信が開始される。非接触式ＩＣカード４００はＲＩＤコマンドを受信すると図３を用いて説明したようにＭＣエリアに特定のコード「12H 」が格納されているか否かの判定と、この判定の結果に応じた処理とが期間Ｐ２で行われる。その後、自身のＩＤコードをリード・ライト装置３００に対して送信する。次に、リード・ライト装置３００から非接触式ＩＣカード４００にリードコマンド５１０を送出すると非接触式ＩＣカード４００はＭＣエリアに「12H 」が格納されている場合にはパスワード５１３が照合一致した場合に限りリードコマンド５１０のアドレス５１２に対応するプログラマブルメモリ４０３のデータをエラーステータス５２１とともにリードデータ５２０としてリード・ライト装置３００に送出する。ＭＣエリアに「12H 」が格納されていなければパスワード５１３の照合の結果にかかわらずアクセスが許可され、リードデータ５２０として送出される。

【００２５】リード・ライト装置３００から非接触式ＩＣカード４００にライトコマンドを送信する場合もリードコマンドの場合と同様である。図８はライトコマンド５３０の構成を示す図である。図に示すようにライトコマンド５３０は、コマンドコード５３１、書き込むべきアドレス５３２、パスワード５３３、ライトデータ列５３４とから構成される。さらに、非接触式ＩＣカード４００からライトコマンド５３０が実行された場合にエラーステータスを返送する。この場合もＭＣエリアに「12

H」が格納されている場合にはコマンドの実行にはパスワード５３３の照合一致が必要になり、MCエリアに「12H」が格納されていなければパスワード５３３が一致しなくてもライトコマンド５３０が実行される。

【００２６】以上説明したように、この実施の形態１ではパスワード付きで送られてきたコマンドについてはMCエリアに特定のコード「12H」が設定されていない場合にはパスワードの照合の結果、一致していなくてもエラーとはならない。従って、同じパスワードで、（どんなパスワードを送っても）プログラマブルメモリ４０３の全エリアのリード及びライトができるので出荷前のメモリの製品テストを容易に行うことができるという効果がある。さらに一旦MCエリアに特定のコード「12H」が設定された場合にはパスワードが一致しなければプログラマブルメモリ４０３のリード及びライト等のアクセスが禁止されるので高いセキュリティを維持することが可能になるという効果がある。

【００２７】実施の形態２．この実施の形態２の基本的構成は実施の形態１と同様である。ただし、以下の点で実施の形態１とは異なっている。すなわち、実施の形態１ではMCエリアに特定コードが設定されていない場合であってもリードコマンド５１０、ライトコマンド５３０を受信したときにパスワードの照合を行っていたが、この実施の形態２ではリードコマンド、ライトコマンドなどを受信したときにパスワードの照合を省略するように制御回路４０４を構成したものである。

【００２８】図９はこの実施の形態２のMCエリアの設定状態によってパスワード照合の実行の有無を決定する場合の動作を示すフローチャートである。図に示すようにMCエリアに特定のコード「12H」が格納されていない場合（ステップＳＴ９０１）にはパスワードの照合をせずにコマンド処理を実行する（ステップＳＴ９０２）。一方、MCエリアに特定のコード「12H」が格納されている場合にはパスワードの照合を行い（ステップＳＴ９０３）、パスワードが一致している場合には（ステップＳＴ９０４）、コマンド処理を実行し、パスワードが一致していなかった場合には（ステップＳＴ９０４）、パスワードエラー処理を実行する（ステップＳＴ９０５）。

【００２９】図１０はMCエリアに特定のコード「12H」が設定されていない場合にリード・ライト装置３００から非接触式ＩＣカード４００に送信するリードコマンド５４０の構成を示す図である。図に示すようにリードコマンド５４０はコマンドコード５４１と、読み出すべきアドレス５４２が送信されるのみであり、パスワードは送信されない。

【００３０】以上のように、この実施の形態２ではMCエリアに特定のコード「12H」が設定されていない場合にはパスワードを送信する必要がなく、また、パスワードの照合の時間も必要なくなるのでテスト時間を短縮することが可能になるという効果がある。

【００３１】実施の形態３．この実施の形態３の基本的構成は実施の形態１と同様である。ただし、プログラマブルメモリ４０３と制御回路４０４とが以下の点で実施の形態１とは異なっている。

【００３２】図１１はこの実施の形態３のプログラマブルメモリ４０３の構成を示すメモリマップを示す図である。図に示すようにこの実施の形態３では製造者エリアMAはMC用のMCエリアと製造者リードパスワード（第２のパスワード、以下MRPと記す）用のMRPエリア（第４の領域）、製造者ライトパスワード（第２のパスワード、以下MWPと記す）用のMWPエリア（第４の領域）とから構成されている。MRP、MWPについては以下に詳細に説明する。

【００３３】図１２は制御回路４０４内に設けられたリードコマンドが入力された場合のエラー処理を実行するためのリードコマンド受信時のエラー信号出力回路（アクセス許可手段）４６０の構成を示す図である。図において、４６１はプログラマブルメモリ４０３の製造者エリアMAに格納されているMRPが入力されたMRPと一致した場合に「H」信号が格納され、一致しない場合には「L」レベル信号が格納されるMRP照合一致フラグ、４６２及び、４６３はオアゲート、４６４はナンドゲート、４６５はアンドゲートを示している。なお、ナンドゲート４６４にはMRP照合一致フラグ４６１からの出力信号とリードコマンドを受信したときに「H」になるリードコマンド信号が入力される。従って、リードコマンドを受信時にMRPが一致した場合にはパスワードエラー及びアドレスエラーがあってもアンドゲート４６５でマスクされてその他のエラーがない場合にはエラー信号はオアゲート４６３からは出力されず、エラー処理は行われない。

【００３４】図１３は制御回路４０４内に設けられた、ライトコマンドが入力された場合のエラー処理を実行するためのライトコマンド受信時のエラー信号出力回路（アクセス許可手段）４７０の構成を示す図である。図において４７１はプログラマブルメモリ４０３の製造者エリアMAに格納されているMWPが入力されたMWPと一致した場合に「H」信号が格納され、一致しない場合には「L」レベル信号が格納されるMWP照合一致フラグを示している。なお、ナンドゲート４７４にはMWP照合一致フラグ４７１からの出力信号とライトコマンドを受信したときに「H」になるライトコマンド信号が入力される。従って、ライトコマンドを受信時にMRPが一致した場合にはパスワードエラー及びアドレスエラーがあってもアンドゲート４７５でマスクされて、その他のエラーがない場合にはエラー信号はオアゲート４７３からは出力されず、エラー処理は行われない。なお、MRP照合一致フラグ４６１及びMWP照合一致フラグ４７１はリセット信号によって「L」レベルにリセット

されるように構成されている。

【００３５】図１４はリード・ライト装置３００と非接触式ＩＣカード４００との間のリード動作時の通信手順を示すシーケンス図である。リード・ライト装置３００から非接触式ＩＣカード４００にＲＩＤコマンドを送出して非接触式ＩＣカード４００がＩＤコードをリード・ライト装置３００に返送してくるまでの動作は実施の形態１で説明したとおりである。なお、非接触式ＩＣカード４００はコミュニケーション開始前にリセットから解除され、コミュニケーション終了時に再びリセットされる。従って、ＭＲＰ照合一致フラグ４６１及びMWP照合一致フラグ４７１は通信開始前には「Ｌ」レベルにリセットされた状態になる。

【００３６】次に、リード・ライト装置３００は非接触式ＩＣカード４００にＭＲＰ照合のためのリードコマンドを送出する。図１５はリードコマンドの構成を示す図である。図に示すようにリードコマンド５５０はコマンドコード５５１、製造者エリアＭＡのＭＲＰのアドレス５５２、ＭＲＰ５５３から構成される。非接触式ＩＣカード４００がこのリードコマンド５５０を受信すると、ＭＲＰを照合して一致した場合には期間Ｐ３でＭＲＰ照合一致フラグ４６１を「Ｈ」にセットし、一致しなかった場合には「Ｌ」のままとする。さらに、このリードコマンド５５０では製造者エリアＭＡのアドレス５５２を指定しているのでアドレス５５２がアクセス禁止領域となり、アドレスエラーを示すエラーステータスをリード・ライト装置３００に返送する。すなわち、この時点では非接触式ＩＣカード４００の外部からはアドレスエラーが発生したリードコマンドと認識される。なお、以上の説明では、リード・ライト装置３００からリードコマンド５５０で直接製造者エリアＭＡのアドレス５５２を指定するようにしたが、予め定められたユーザエリアＵＡ以外の任意のアドレスをリード・ライト装置３００から非接触式ＩＣカード４００に送信するようにしても良い。この場合には非接触式ＩＣカード４００は予め定められたアドレスをリードコマンドとして受信した場合に製造者エリアＭＡのＭＲＰのアドレスのリードアクセスとして認識するように構成する。このように構成することで、必ずしもユーザエリアＵＡの近くの領域である製造者エリアＭＡの実アドレスを送信しなくても良いのでさらに高いセキュリティーを得ることができる。

【００３７】次に、リード・ライト装置３００からリードコマンド５５０を非接触式ＩＣカード４００に送信するとＭＲＰ照合一致フラグ４６１が「Ｈ」にセットされている場合には、パスワードが不一致であってもエラー処理は行われずにプログラマブルメモリ４０３のすべてのアドレスのリードが許可され、対応するアドレスのデータがリード・ライト装置３００に送信される。なお、ＭＲＰ照合一致フラグ４６１が「Ｌ」のままの場合には、パスワードが一致した場合のみプログラマブルメモリ４０３のアドレスＡＤ０からアドレスＡＤ５の領域のリードが許可される。

【００３８】図１６はリード・ライト装置３００と非接触式ＩＣカード４００との間のライト動作時の通信手順を示すシーケンス図である。リード・ライト装置３００から非接触式ＩＣカード４００にＲＩＤコマンドを送出して非接触式ＩＣカード４００がＩＤコードをリード・ライト装置３００に返送してくるまでの動作は実施の形態１で説明したとおりである。

【００３９】次に、リード・ライト装置３００は非接触式ＩＣカード４００にMWP照合のためのリードコマンドを送出する。図１７はこのリードコマンドの構成を示す図である。図に示すようにリードコマンド５６０はコマンドコード５６１、製造者エリアＭＡのMWPのアドレス５６２、MWP５６３から構成される。非接触式ＩＣカード４００がこのリードコマンド５６０を受信すると、MWPを照合して一致した場合には期間Ｐ４でMWP照合一致フラグ４７１を「Ｈ」にセットし、一致しなかった場合には「Ｌ」のままとする。さらに、このリードコマンド５６０では製造者エリアＭＡのアドレス５６２を指定しているのでアクセスアドレスは禁止領域となり、アドレスエラーを示すエラーステイタスをリード・ライト装置３００に返送する。すなわち、この時点では非接触式ＩＣカード４００の外部からはアドレスエラーが発生したリードコマンドと認識される。

【００４０】次にリード・ライト装置３００からライトコマンド５６０を非接触式ＩＣカード４００に送信するとMWP照合一致フラグ４７１が「Ｈ」にセットされている場合には、パスワードが不一致であってもエラー処理は行われずにプログラマブルメモリ４０３のすべてのアドレスの書き込みが許可され、対応するアドレスにデータが書き込まれる。その後、リード・ライト装置３００にエラーステータスデータを送出し、エラーの状態および書き込みが終了したことを通知する。なお、MWP照合一致フラグ４７１が「Ｌ」のままである場合には、各エリアのパスワードが一致した場合のみアドレスＡＤ０からアドレスＡＤ５の領域の書き込みが許可される。

【００４１】以上のように、この実施の形態３では、例えば、不良解析などのためＭＣエリアに特定コード「12Ｈ」が設定された後でも一定の手続きを経てパスワードエラー、アドレスエラーを無視することができるので高いセキュリティーを保ちつつ不良解析時のテストを容易にすることができる効果がある。

【００４２】実施の形態４．この実施の形態４は上述した実施の形態３と基本的構成は同じである。ただし以下の点で実施の形態３とは異なっている。

【００４３】図１８はこの実施の形態４の非接触式ＩＣカード４００の制御回路４０４内のリードコマンド受信時のエラー信号出力回路（アクセス許可手段）４６０ａの構成を示す図である。図において、４６６はＭＲＰ照

合後に受信したリードコマンドの回数をカウントするコマンドカウンタ（カウント手段）、４６７はカウントされたコマンドの回数が所定値以上であるか否かを判定する比較回路、４６５ａは３入力ナンドゲートを示している。なお、図１２と同一の部分には同一の符号を付し、重複する説明は省略する。

【００４４】図１９はリード・ライト装置３００と非接触式ＩＣカード４００との間の通信手順を示すシーケンス図である。図に示すようにＲＩＤコマンドをリード・ライト装置３００が非接触式ＩＣカード４００に送って通信が開始されてから期間Ｐ３後に非接触式ＩＣカード４００がエラーステータスを返送するまでは実施の形態３と同様である。その後リード・ライト装置３００から非接触式ＩＣカード４００にリードコマンドが送られるとコマンドカウンタ４６６がカウントし、カウント値を出力する。コマンドカウンタ４６６がｎを越えるカウント値を出力すると比較回路４６７は「H」レベルの信号を出力する。すなわち、ＭＲＰ照合一致フラグ４６１がセットされてからｎ個（ｎは整数）のリードコマンドまではパスワードエラー、アドレスエラーは有効であるがｎ＋１回目以降のリードコマンドはパスワードエラー、アドレスエラーがあってもエラー信号は発生されずに実行される。従って、この実施の形態４ではｎ回のリードコマンドがあった後に始めてリードコマンドがパスワードの照合一致を必要とせずに実行されることを知らない第３者に対するセキュリティーを向上させることができる。

【００４５】同様にしてライトコマンドに対してもｎ回のＭＷＰの照合フラグがセットされた後、ｎ個（ｎは整数）のライトコマンドまではパスワードエラー、アドレスエラーは有効であるが、ｎ＋１回目以降のライトコマンドはパスワードエラー、アドレスエラーがあってもエラー信号は発生されずに実行されるように構成される。図２０はこの場合のエラー信号出力回路（アクセス許可手段）４７０ａの構成を示す図であり、４７６はＭＷＰ照合一致フラグ４７１がセットされた後にライトコマンドの数をカウントするコマンドカウンタ（カウント手段）、４７７はコマンドカウンタ４７６から出力されるライトコマンドの数がｎ個に達したら「H」レベルの信号を出力する比較回路である。従って、この実施の形態４ではｎ回のライトコマンドがあった後に始めてライトコマンドがパスワードの照合一致を必要とせずに実行されることを知らない第３者に対するセキュリティーを向上させることができる。

【００４６】以上説明したように、この実施の形態４ではさらに高いセキュリティーを維持しつつメモリテストを容易にできる効果がある。

【００４７】実施の形態５．この実施の形態５は上述した実施の形態４と基本的構成は同じである。ただし以下の点で実施の形態４とは異なっている。すなわち、実施

の形態４では比較回路４６７及び比較回路４７７は所定のカウント値ｎを越えた場合に、「H」レベルの信号を出力するように構成した。しかしフラグがセットされてからコマンドの回数がｉ以上ｊ以下の場合に（ｉ、ｊは整数）、「H」レベルの信号を維持し、ｊ＋１回目以降は「L」レベルの信号を出力するようにしても良い。この場合にはフラグがセットされてからｉ回目からｊ回目までのリードコマンドまたはライトコマンドのアクセスはパスワードが一致しなくても許可される。そしてｊ＋１回目以降のコマンドはパスワードの照合の結果一致することが必要になる。

【００４８】以上説明したように、この実施の形態５によれば、さらにセキュリティーを高くしつつ容易にメモリのテストをすることができる効果がある。

【００４９】実施の形態６．この実施の形態６は上述した実施の形態３と基本的構成は同様である。ただし以下の点で実施の形態３とは異なっている。すなわち、実施の形態３では、ＭＲＰ、ＭＷＰを独立して設定したが、この実施の形態６ではＭＲＰ、ＭＷＰの両方を照合して、両方とも一致すれば、それ以降はリードコマンド、ライトコマンドの両方をプログラマブルメモリ４０３のすべてのエリアに対してパスワードが一致しなくてもエラーとなることなしに実行することができる。

【００５０】図２１は制御回路４０４のエラー信号発生回路（アクセス許可手段）４８０の構成を示す回路図である。図において、４８１はＭＲＰ照合一致フラグ４６１の出力とＭＷＰ照合一致フラグ４７１の出力とが入力されるアンドゲートである。なお、図１２、図１３と同一の部分には同一の符号を付し、重複する説明は省略する。

【００５１】図２２はこの実施の形態６のリード・ライト装置３００と非接触式ＩＣカード４００との間の通信手順を示すシーケンス図である。図に示すようにＩＤコードの確認後にＭＲＰ照合のためのリードコマンドをリード・ライト装置３００から非接触式ＩＣカード４００に送ってＭＲＰの照合を行い、次にＭＷＰ照合のためのリードコマンドを送ってＭＷＰの照合を行う。ＭＲＰとＭＷＰの両方が、照合の結果、一致した場合にリード・ライト装置３００からのリードコマンド及びライトコマンドがパスワードＰＷ１からＰＷ５の照合の結果にかかわらずプログラマブルメモリ４０３のすべてのアドレスに対して実行できる。また、実施の形態２で説明したようにパスワードの照合を省略するようにすることもできる。

【００５２】実施の形態７．この実施の形態７は上述した実施の形態６と基本的構成は同じである。ただし以下の点で実施の形態６とは異なっている。すなわち、上述した実施の形態６ではＭＲＰとＭＷＰの照合の結果、両方とも一致した場合、その後は、リードコマンド及びライトコマンドがパスワードＰＷ１からＰＷ５の照合の結

果、一致していなくても実行するように構成したが、この実施の形態７ではＭＲＰとＭＷＰの照合の結果、両方とも一致した場合、その後、所定のｎ個（ｎは整数）のコマンドはパスワードの照合が必要であるが、ｎ＋１回目以降のリードコマンド及びライトコマンドはパスワードの照合の一致を必要とせずに実行することができるように構成している。

【００５３】図２３はこの実施の形態７の非接触式ＩＣカード４００の制御回路４０４内に設けられたエラー信号出力回路（アクセス許可手段）４８０ａの構成を示すブロック図である。図２１に示すエラー信号出力回路４８０と同一の部分には同一の符号を付し、重複する説明は省略する。図において、４８４はＭＲＰ照合一致フラグ４６１とＭＷＰ照合一致フラグ４７１の両方が「Ｈ」にセットされた後、非接触式ＩＣカード４００が受信したリードコマンドまたはライトコマンドの数をカウントするコマンドカウンタ（カウント手段）、４８２はコマンドカウンタ４８４から出力されるカウント値がｎ（ｎは整数）を越えると「Ｈ」レベルの信号を出力する比較回路、４８３はＭＲＰ照合一致フラグ４６１、ＭＷＰ照合一致フラグ４７１、及び比較回路４８２の出力が入力される３入力ナンドゲートである。

【００５４】次に動作について説明する。図２４はこの実施の形態７の非接触式ＩＣカード４００とリード・ライト装置３００との間の通信手順を示すシーケンス図である。同図に示すようにＭＲＰの照合及びＭＷＰの照合については実施の形態６と同様である。

【００５５】ＭＲＰの照合及びＭＷＰの照合の結果、両者とも一致している場合にはＭＲＰ照合一致フラグ４６１、ＭＷＰ照合一致フラグ４７１がともに「Ｈ」にセットされる。そしてその後リードコマンドまたはライトコマンドがリード・ライト装置３００から送られてくるとコマンドカウンタ４８４は入力されたコマンドの数をカウントして、カウント値を出力する。比較回路４８２は入力されたコマンドの数がｎを越えると「Ｈ」レベル信号を出力する。このため、ｎ＋１回目からのコマンドについてはパスワードの照合結果に関係なくリード・ライト装置３００からのリードコマンド及びライトコマンドがプログラマブルメモリ４０３のすべてのアドレスに対して実行できる。また、実施の形態５で説明したようにＭＲＰ照合一致フラグ４６１、ＭＷＰ照合一致フラグ４７１がセットされた後、ｉ回目からｊ回目（ｉ、ｊは整数）までのコマンドのみ許可するようにしても良い。さらに、実施の形態２で説明したようにパスワードの照合を省略するようにすることもできる。

【００５６】以上説明したように、この実施の形態７では、ＭＲＰとＭＷＰが両方とも一致してはじめてメモリのアクセスが許可されるのでさらにセキュリティーを高くできるという効果がある。

【００５７】

【発明の効果】以上のように、請求項１記載の発明によれば、アクセス許可手段を、メモリの所定の領域に所定のコードが格納されているときは、第１のパスワードが一致している場合には外部装置からのメモリの第２の領域のアクセスを許可し、所定のコードが格納されていない場合には、パスワード照合手段による第１のパスワードの照合の結果にかかわらず外部装置からのメモリの第１及び第２の領域へのアクセスを許可するように構成したので、高いセキュリティーを維持しつつメモリのテストを容易にすることができる効果がある。

【００５８】請求項２記載の発明によれば、アクセス許可手段を、メモリの所定の領域に所定のコードが格納されているときは、パスワード照合手段による照合の結果、第１のパスワードが一致している場合に外部装置からのメモリの第２の領域のアクセスを許可し、所定のコードが格納されていない場合には、第１のパスワードの照合をせずに外部装置からのメモリの第１及び第２の領域へのアクセスを許可するように構成したので、高いセキュリティーを維持しつつメモリのテストを容易、高速にすることができる効果がある。

【００５９】請求項３記載の発明によれば、判断手段を、メモリの所定の領域に所定のコードが格納されているか否かを、外部装置からのＩＤコード要求のコマンドを受信してから外部装置にＩＤコードを送出するまでの期間に判断するように構成したので所定のコードが格納されているか否かの判断を確実にして高いセキュリティーを維持できる効果がある。

【００６０】請求項４記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、第２のパスワードが一致した場合には外部装置からのメモリの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティーを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【００６１】請求項５記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、第２のパスワードが一致し、且つ、カウント手段によってカウントされたコマンドの数が所定の数以上である場合には外部装置からのメモリの第１の領域及び第２の領域へのアクセスを第１のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティーを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【００６２】請求項６記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、第２のパスワードが一致し、且つ、外部装置から送られてきたコマンドの数が第１の所定数以上で、且つ、第２の所定数以下である場合に、外部装置からのメモリの第１の領域及び第２の領域へのア

19

クセスを第１のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティーを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【００６３】請求項７記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、リードパスワードが一致した場合には外部装置からのメモリの第１の領域及び第２の領域のデータの読み出しを第１のパスワードの照合の一致を必要とせずに許可し、ライトパスワードが一致した場合には外部装置からのメモリの第１の領域及び第２の領域へのデータの書き込みを第１のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティーを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【００６４】請求項８記載の発明によれば、アクセス許可手段を、メモリの所定領域に所定のコードが格納されている場合であっても、リードパスワード及びライトパスワードの両方が一致した場合には外部装置からのメモリの第１の領域及び第２の領域の読み出し及び書き込みの両方を第１のパスワードの照合の一致を必要とせずに許可するように構成したので、高いセキュリティーを維持しつつメモリのテストをさらに容易にすることができる効果がある。

【図面の簡単な説明】

【図１】　この発明の実施の形態１の非接触式ＩＣカードの通信システムを示す図である。

【図２】　実施の形態１の非接触式ＩＣカードのプログラマブルメモリのメモリマップを示す図である。

【図３】　実施の形態１のリード・ライト装置と非接触式ＩＣカードとの間の通信手順を示すシーケンス図である。

【図４】　実施の形態１においてコマンドを非接触式ＩＣカードが受信したときのエラー処理を実行する制御回路内のエラー信号生成回路の構成を示す図である。

【図５】　実施の形態１のリード・ライト装置から非接触式ＩＣカードにリードコマンドを転送した場合の通信手順を示すシーケンス図である。

【図６】　リードコマンドの構成を示す図である。

【図７】　リードコマンドがリード・ライト装置から送信されてきた場合に非接触式ＩＣカードからリード・ライト装置に送信されるリードデータの構成を示す図である。

【図８】　ライトコマンドの構成を示す図である。

【図９】　この発明の実施の形態２のＭＣエリアの設定状態によってパスワード照合の実行の有無を決定する場合動作を示すフローチャートである。

【図１０】　実施の形態２においてＭＣエリアに特定のコードが設定されていない場合にリード・ライト装置から非接触式ＩＣカードに送信するリードコマンドの構成

20

を示す図である。

【図１１】　この発明の実施の形態３のプログラマブルメモリの構成を示すメモリマップを示す図である。

【図１２】　実施の形態３の制御回路内に設けられたリードコマンドが入力された場合のエラー処理を実行するためのリードコマンド受信時のエラー信号出力回路の構成を示す図である。

【図１３】　実施の形態３の制御回路内に設けられたライトコマンドが入力された場合のエラー処理を実行するためのライトコマンド受信時のエラー信号出力回路の構成を示す図である。

【図１４】　実施の形態３におけるリード・ライト装置と非接触式ＩＣカードとの間のリード動作時の通信手順を示すシーケンス図である。

【図１５】　ＭＲＰ照合のためのリードコマンドの構成を示す図である。

【図１６】　実施の形態３におけるリード・ライト装置と非接触式ＩＣカードとの間のライト動作時の通信手順を示すシーケンス図である。

【図１７】　ＭＷＰ照合のためのリードコマンドの構成を示す図である。

【図１８】　この発明の実施の形態４の非接触式ＩＣカードの制御回路内のリードコマンド受信時のエラー信号出力回路の構成を示す図である。

【図１９】　実施の形態４におけるリード・ライト装置と非接触式ＩＣカードとの間の通信手順を示すシーケンス図である。

【図２０】　実施の形態４のエラー信号出力回路の構成を示す図である。

【図２１】　この発明の実施の形態６のエラー信号発生回路の構成を示す図である。

【図２２】　実施の形態６におけるリードライト・装置と非接触式ＩＣカードとの間の通信手順を示すシーケンス図である。

【図２３】　この発明の実施の形態７の非接触式ＩＣカードの制御回路内に設けられたエラー信号出力回路の構成を示す図である。

【図２４】　実施の形態７における非接触式ＩＣカードとリード・ライト装置との間の通信手順を示すシーケンス図である。

【図２５】　従来の非接触式ＩＣカードに用いられるプログラマブルメモリ内蔵のＬＳＩのメモリマップを示す図である。

【図２６】　従来の非接触式ＩＣカード通信システムの構成を示す図である。

【図２７】　従来のリード・ライト装置と非接触式ＩＣカードとの間の通信手順を示すシーケンス図である。

【符号の説明】

３００．リード・ライト装置（外部装置）、４００　非接触式ＩＣカード（通信装置）、４０３　プログラマブ

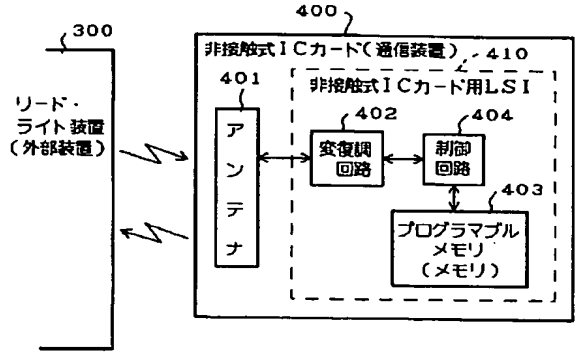
21

ルメモリ（メモリ）、４５０，４６０，４６０ａ，４７０，４７０ａ，４８０，４８０ａ　エラー信号出力回路（アクセス許可手段）、４５１　パスワード照合回路（パスワード照合手段）、４５４　ＭＣ設定フラグ（判

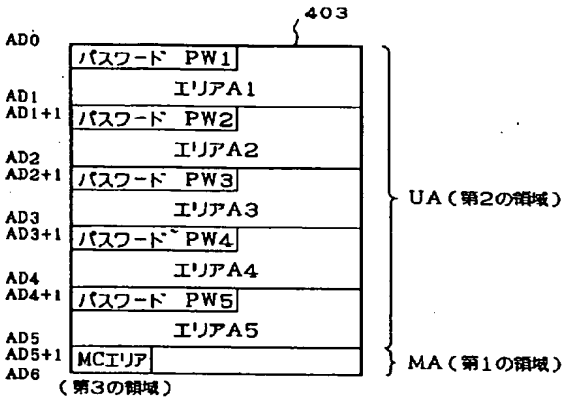
22

断手段）、４６６，４７６，４８４　コマンドカウンタ（カウント手段）、ＭＡ　製造者エリア（第１の領域）、ＵＡ　ユーザエリア（第２の領域）。

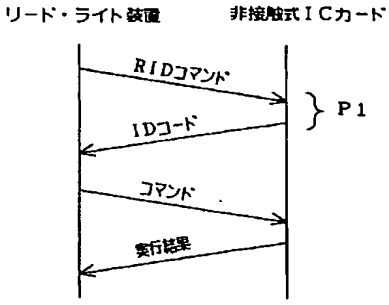
【図１】



【図２】

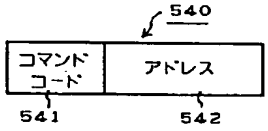


【図３】

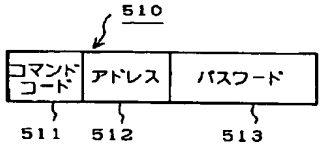


MA：製造者エリア（第1の領域）
UA：ユーザエリア（第2の領域）

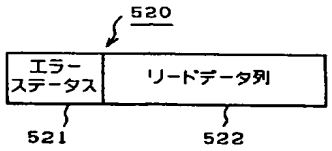
【図１０】



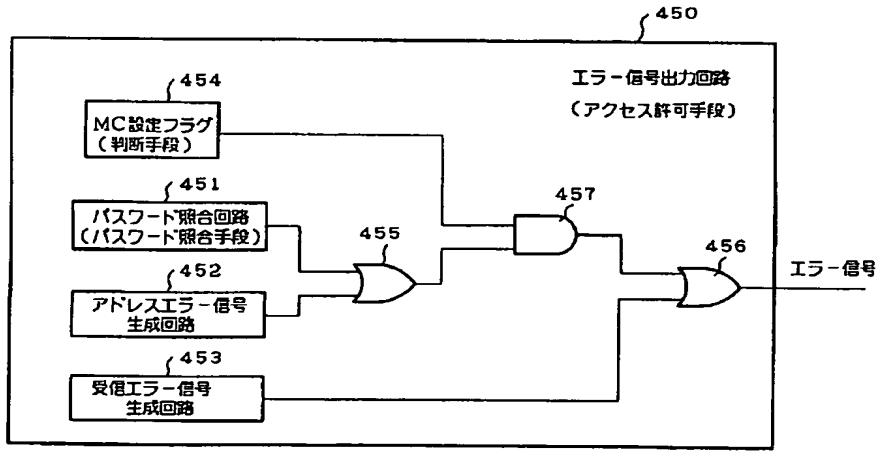
【図６】



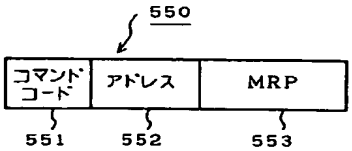
【図７】



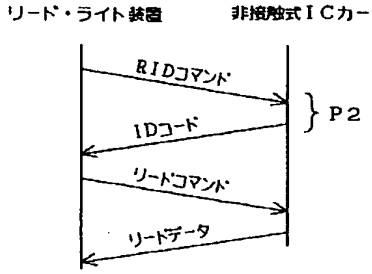
【図４】



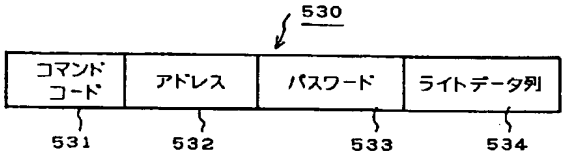
【図１５】



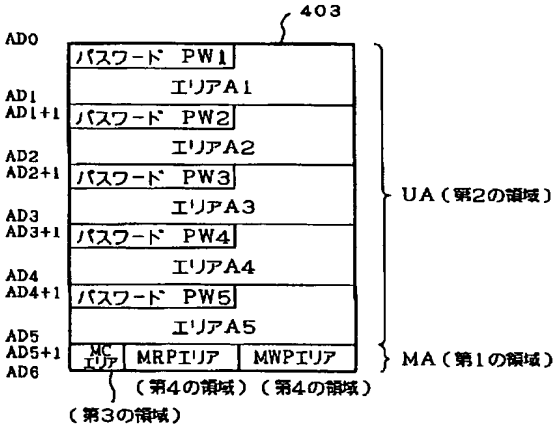
【図５】



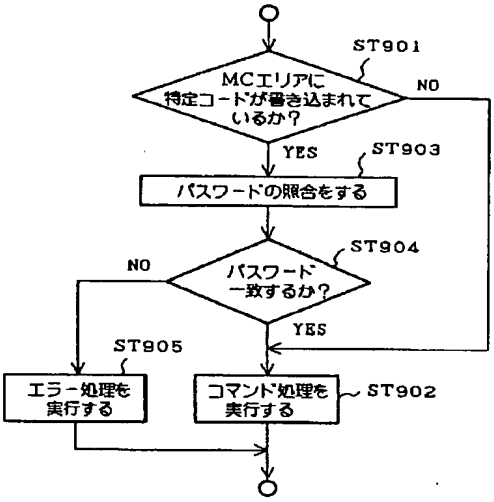
【図８】



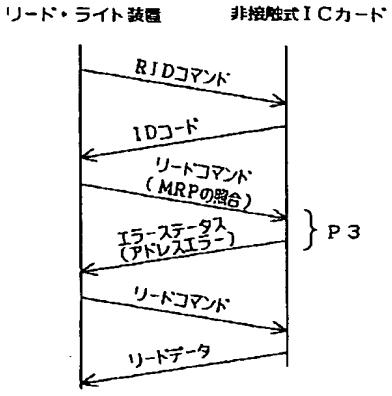
【図１１】



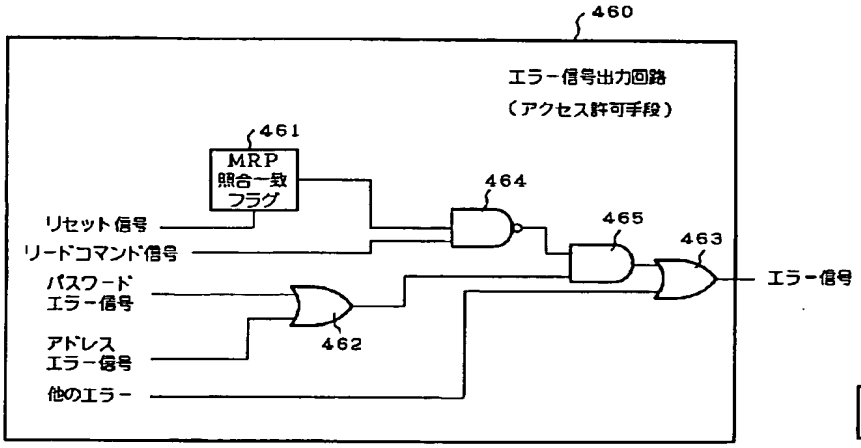
【図９】



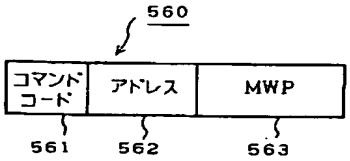
【図１４】



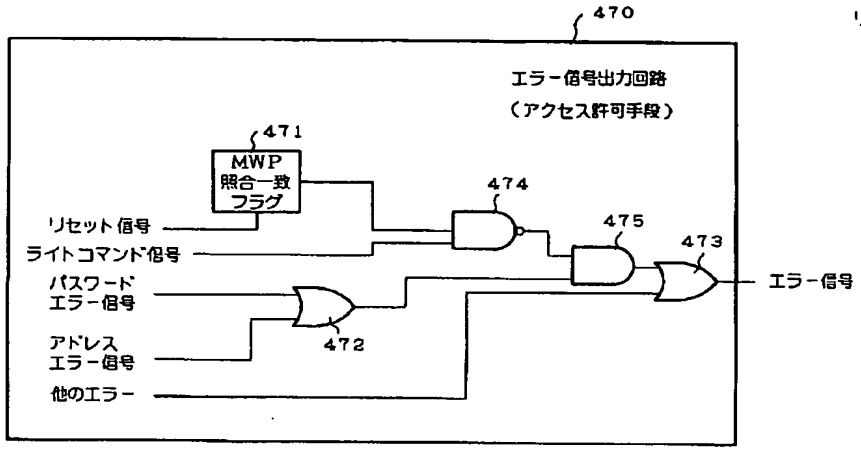
【図１２】



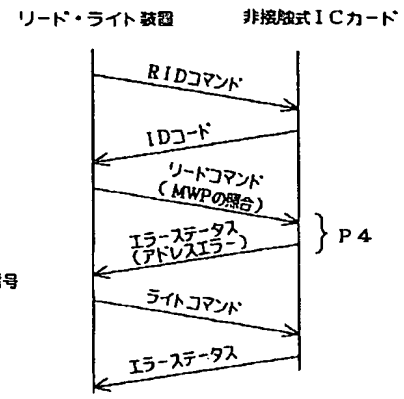
【図１７】



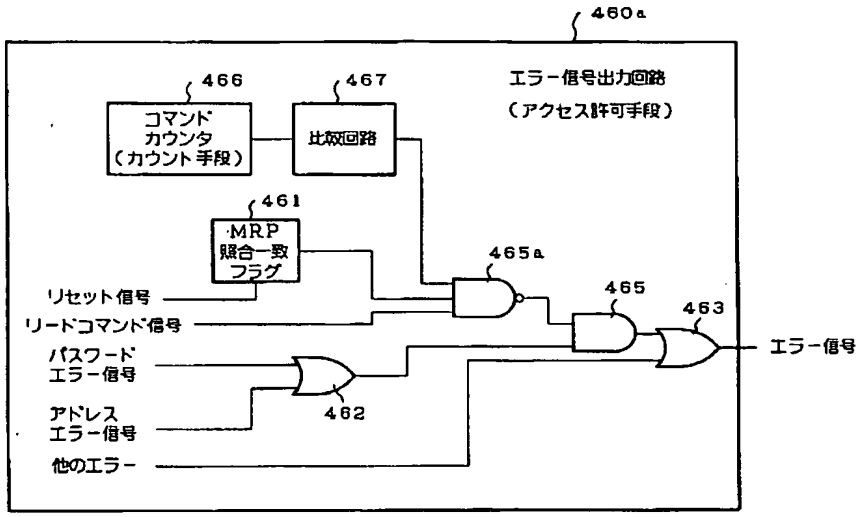
【図１３】



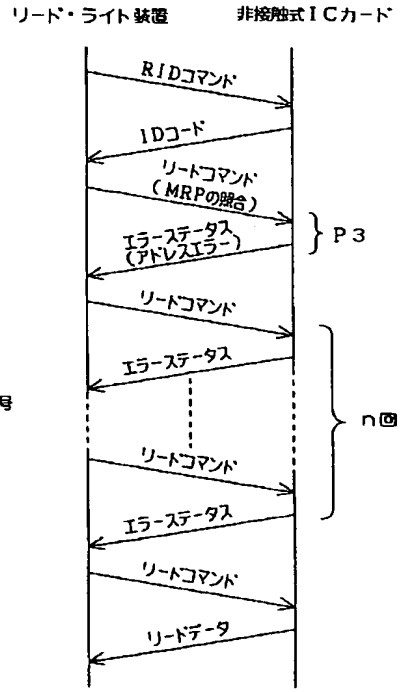
【図１６】



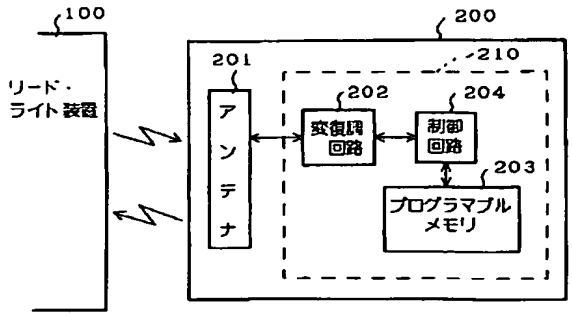
【図１８】



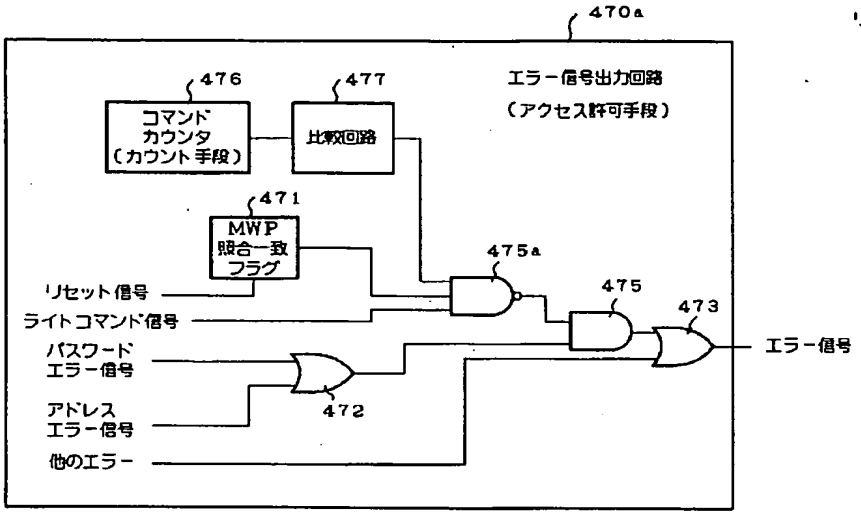
【図１９】



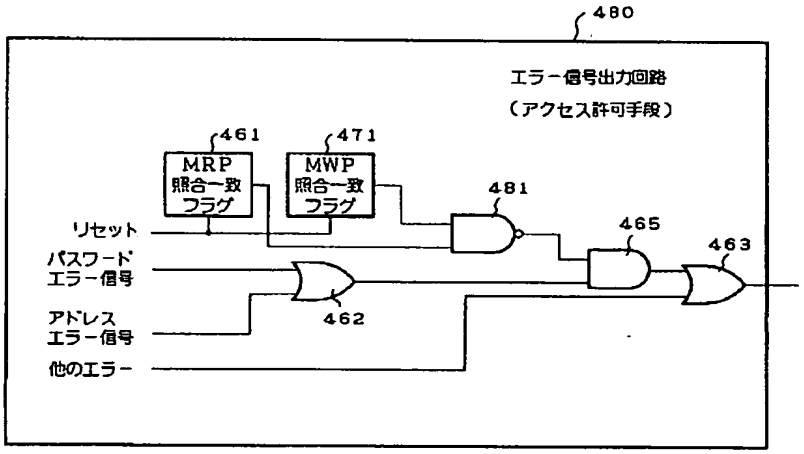
【図２６】



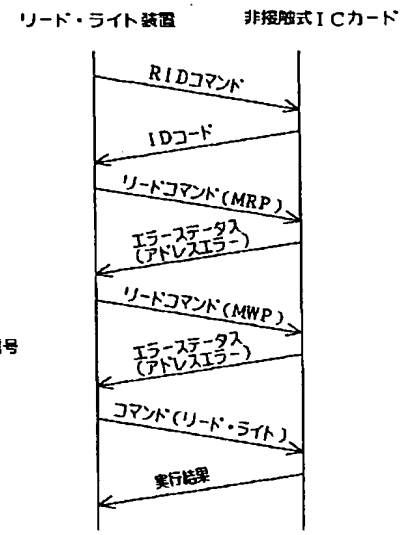
【図２０】



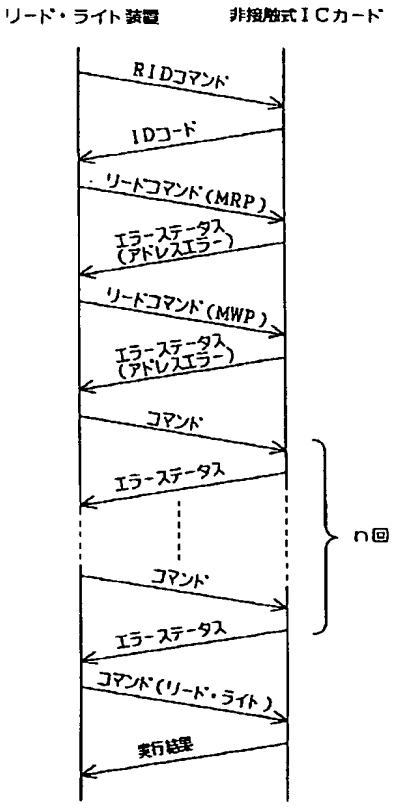
【図２１】



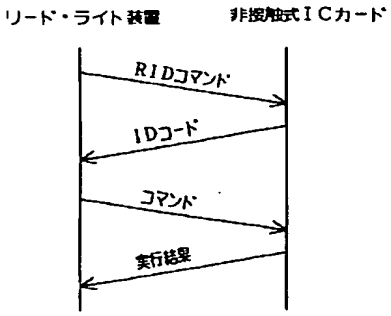
【図２２】



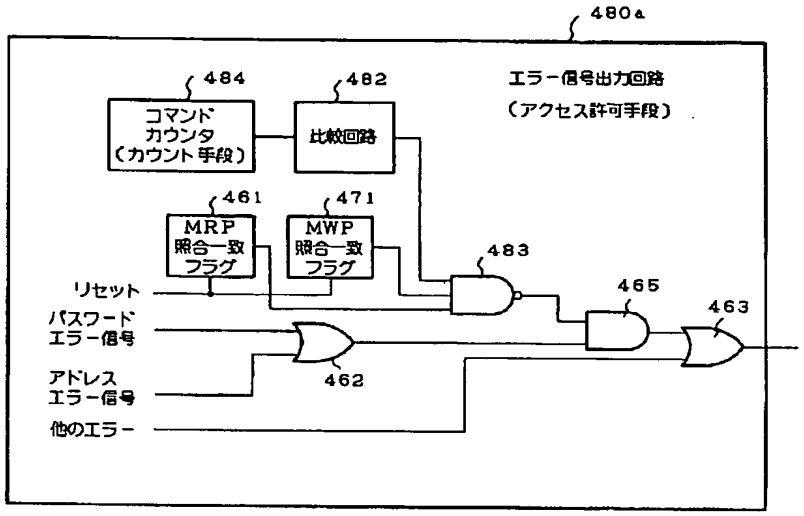
【図２４】



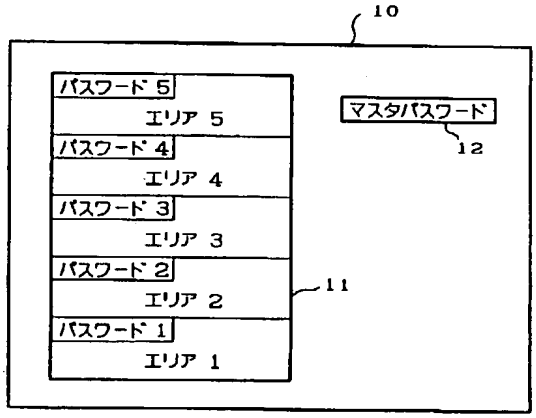
【図２７】



【図２３】



【図２５】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	Ｆ Ｉ		技術表示箇所
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ　9/00	６７３Ａ	
				６７３Ｅ	